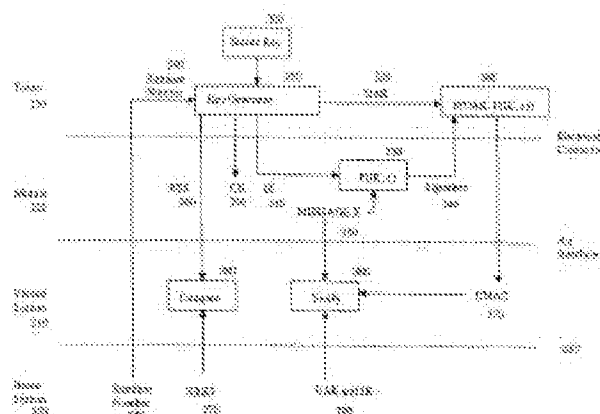


Patent number: JP2004533174 (T)
Publication date: 2004-10-28
Inventor(s):
Applicant(s):
Classification:
- **international:** H04L29/06; H04L9/32; H04M3/00; H04W12/06; H04L29/06; H04L9/32; H04M3/00; H04W12/00; (IPC1-7): H04L9/32; H04M3/00; H04Q7/38
- **europaean:** H04L29/06S12; H04L9/32R; H04Q7/38A
Application number: JP20020592675T 20020521
Priority number(s): US20010863139 20010522; WO2002US16103 20020521

Abstract of correspondent: **WO 02096150 (A1)**

Methods and apparatus are presented for providing local authentication of subscribers travelling outside their home systems. A subscriber identification token (230) provides authentication support by generating a signature (370) based upon a key that is held secret from a mobile unit (220). A mobile unit (220) that is programmed to wrongfully retain keys from a subscriber identification token (230) after a subscriber has removed his or her token is prevented from subsequently accessing the subscriber's account.



【特許請求の範囲】**【請求項 1】**

下記を具備する、通信システムにおいて加入者のローカル認証を提供するための加入者識別モジュール：

メモリ、及び；

該メモリ内に蓄積された 1 セットの命令を実施するように構成されたプロセッサ、該命令のセットは下記を行う：

受信されたチャレンジに応じて複数のキーを発生する；

該複数のキーからの第 1 のキーに基づいた初期値を発生する；

該初期値を受信された信号と連結し、入力値を形成する、該受信された信号は該加入者識別モジュールに通信的に連結された通信ユニットから送信される、及び該受信された信号は該複数のキーからの第 2 のキーを使用して該通信ユニットにより発生され、該第 2 のキーは該加入者識別モジュールから該通信ユニットに通信された；

認証信号を形成するために該入力値をハッシュする；及び

該通信ユニットを介して該通信システムに該認証信号を送信する。

【請求項 2】

該入力値をハッシュすることは該安全ハッシュアルゴリズム（SHA-1）に従って実行される、請求項 1 記載の装置。

【請求項 3】

該初期値を発生することは該第 1 のキーをパッドすることを具備する、請求項 1 記載の装置。

【請求項 4】

該初期値を発生することは定数値に、パッドされた第 1 のキー ビットワイズを付加することをさらに具備する、請求項 3 記載の装置。

【請求項 5】

該受信された信号は下記を行うことにより該通信ユニットで発生される、請求項 1 記載の装置：

該加入者識別モジュールから該第 2 のキーを受信する；

該第 2 のキーに基づいたローカル初期値を発生する；

ローカル入力値を形成するために該ローカル初期値とメッセージとを連結する；

該受信された信号を形成するために該ローカル入力値をハッシュする；及び

該加入者識別モジュールに該受信された信号を送信する。

【請求項 6】

該ローカル初期値を発生することは該第 2 のキーをパッドすることを具備する、請求項 5 記載の装置。

【請求項 7】

該ローカル初期値を発生することは第 2 の定数値に、パッドされた第 2 のキー ビットワイズを付加することをさらに具備する、請求項 6 記載の装置。

【請求項 8】

下記を具備する、加入者識別モジュール：

キー発生素子；及び

該キー発生素子から秘密キーを、及び移動体ユニットから情報を、受信するように構成された、及び該移動体ユニットに送出されるであろう署名を発生するようにさらに構成された署名発生器、該署名は該秘密キーを該移動体ユニットからの該情報と連結することにより及び該連結された秘密キー及び情報をハッシュすることにより発生される。

【請求項 9】

該キー発生素子は下記を具備する、請求項 8 記載の加入者識別モジュール：

メモリ；及び

該メモリ内に蓄積された 1 セットの命令を実行するように構成されたプロセッサ、ここで該命令のセットは複数の臨時キーを形成するために入力値上で暗号変換を実行する。

【請求項 1 0】

該暗号変換は固定キーを使用して実行される、請求項 9 記載の加入者識別モジュール。

【請求項 1 1】

通信ユニットと対話するように構成された加入者識別モジュールを具備する、通信システムにおいて加入者の安全なローカル認証を提供するための装置、ここで該加入者識別モジュールは下記を具備する：

受信された値と秘密の値とから複数のキーを発生するためのキー発生器、ここで該複数のキーからの少なくとも 1 つの通信キーは該通信ユニットに伝送される及び該複数のキーからの少なくとも 1 つの秘密キーは該通信ユニットに伝送されない；及び

該少なくとも 1 つの秘密キーの 1 形式を認可メッセージと共にハッシュすることから認可信号を発生するための署名発生器、ここで認可メッセージは該少なくとも 1 つの通信キーの 1 形式を使用して該通信ユニットにより発生される。

10

【請求項 1 2】

該加入者識別モジュールは該通信ユニットに挿入されるように構成される、請求項 1 1 記載の装置。

【請求項 1 3】

該少なくとも 1 つの通信キーは統合性キーを具備する、請求項 1 1 記載の装置。

【請求項 1 4】

ハッシュすることは S H A - 1 に従って実行される、請求項 1 1 記載の装置。

【請求項 1 5】

下記を具備する、加入者識別装置を使用して加入者の認証を提供するための方法：

複数のキーを発生する；

該加入者識別装置に通信的に連結された通信装置に該複数のキーから、少なくとも 1 つのキーを送信する及び該複数のキーからの少なくとも 1 つのキーで秘密を保持する；

該通信装置に送信された該少なくとも 1 つのキー及び送信メッセージの両者を使用して該通信装置で署名を発生する、ここで発生することは該少なくとも 1 つのキーと該送信メッセージとから形成された連結値をハッシュすることにより実施される；

該加入者識別装置に該署名を送信する；

該加入者識別装置で該署名を受信する；

該受信された署名から一次署名を発生する、ここで該発生することは該少なくとも 1 つの秘密キーから形成された連結値と該通信装置から受信された該署名とをハッシュすることにより実施される；及び

20

通信システムに該一次署名を伝達する。

【請求項 1 6】

ハッシュすることは S H A - 1 に従って実施される、請求項 1 5 記載の方法。

【請求項 1 7】

下記を具備する、無線通信システムにおいて加入者を認証するための装置、ここで該装置は該無線通信システム内で動作する移動局に通信的に連結されることができる：

メモリ；及び

該メモリ内に蓄積された 1 セットの命令を実施するように構成されたプロセッサ、該命令のセットは該移動局から秘密を保持されたキーに基づいた一次署名と該移動局から受信される二次署名とを選択的に発生する。

30

40

【発明の詳細な説明】**【技術分野】****【0 0 0 1】**

本発明は通信システムに関し、そしてより詳しくは、通信システム加入者のローカル認証(local authentication)に関する。

【背景技術】**【0 0 0 2】**

無線通信の分野は、例えば、コードレス電話機、ページング、無線ローカルループ、個人

50

ディジタル補助(assistants)(PDA)、インターネット電話、及び衛星通信システムを含む多くのアプリケーションを有する。特に重要なアプリケーションは移動体加入者用のセルラ電話システムである。この中で使用されるように、術語“セルラ”システムはセルラ及び個人通信サービス(PCS)の両周波数を含む。種々の大気中送信インターフェイスは、例えば、周波数分割多重アクセス(FDMA)、時分割多重アクセス(TDMA)、及び符号分割多重アクセス(CDMA)を含むそのようなセルラ電話システムのために開発された。それに関して、種々の国内及び国際標準は、例えば、進歩した移動電話サービス(AMPS)、移動体用グローバルシステム(GSM)、及び暫定標準95(IS-95)を含んで確立された。特に、IS-95とその派生物、IS-95A、IS-95B、ANSI-JSTD-008(この中ではしばしば集合的にIS-95と呼ばれる)、及びデータ用に提案された高速データシステム(high-data-rate system)等は、電気通信工業協会(TTA)及び他の周知の標準団体により公布されている。

10

【0003】

IS-95標準の使用に従って構成されたセルラ電話システムは、高度に効率的なそして強いセルラ通信サービスを提供するためにCDMA信号処理技術を使用する。実質的にIS-95標準の使用に従って構成された典型的なセルラ電話システムは米国特許番号第5,103,459号及び第4,901,307号に記述され、それらは本発明の譲受人に譲渡され、引用されてこの中に組み込まれる。CDMA技術を使用している典型的なシステムは、TTAにより発行された、cdma2000ITU-R無線送信技術(RTT)候補者寄託(この中でcdma2000と呼ばれる)である。cdma2000のための標準はIS-2000の草稿版内に与えられて、TTAにより認可された。cdma2000案は多くの意味で(in many ways)IS-95システムと一致する。もう1つのCDMA標準は、第3世代パートナーシップ・プロジェクト“3GPP”、文書番号第3G-TS25.211号、第3G-TS25.212号、第3G-TS25.213号、及び第3G-TS25.214号内に具体化されたように、W-CDMA標準である。

20

【0004】

世界の大部分において電気通信サービスの偏在する急増と一般大衆の増加する移動性とがあるとなれば、彼等が加入者のホームシステムの領域外に旅行している間も加入者に通信サービスを提供することが望ましい。この要求を満足させる1方法は、GSMシステム内の加入者識別モジュール(SIM)のような、識別トークン(token)の使用であり、ここで加入者はGSM電話機に挿入可能なSIMカードを割り当てられる。SIMカードは、SIMカードを移動体電話機に挿入している当事者のビリング(billing)情報を識別するのに使用される情報を運ぶ。次世代SIMカードはUSIM(UTMS-SIM)カードと名前を換えられた(renamed)。CDMAシステムでは、識別トークンは着脱可能型ユーザ・インターフェイス・モジュール(R-UIM)と呼ばれて、同じ目的を達成する。そのような識別トークンの使用は、加入者が彼等の個人的移動体電話機無しに旅行することを可能とし、それは訪問先の(visited)環境内では使用されない周波数上で動作できるように、また新しい口座を開設する際にコストを発生すること無くローカルに使用可能な移動体電話を使用するように構成されることができる。

30

【0005】

便利ではあるが、加入者の口座情報にアクセスするためのそのような識別トークンの使用は不安定(insecure)の可能性がある。一般に、そのような識別トークンは、メッセージ暗号化のために使用される暗号キーまたは加入者を識別するための認証キーのような秘密情報を移動体電話機に送信するようにプログラムされる。口座情報の盗難を予想している(contemplating)人は、識別トークンが抹消された(removed)後にも秘密情報を保有する(retain)ように、または移動体電話機の正当な使用の間は他の蓄積ユニットに秘密情報を送信するように移動体電話機をプログラミングすることにより彼等の目的を達成することができる。この手法で手を加えられた(tampered)移動体電話機は以降“ローグ・シェル(rogue shell)”と呼ばれるであろう。よって、通信サービスにアクセスするために上述の秘密情報の使用をな容易とする(facilitating)一方で、識別トークン上に蓄積された秘密

40

50

情報の安全性を保護することに最近の要求がある。

【0006】

[概要]

彼等のホームシステム外での加入者ローミングに安全な認証を提供するための新規な方法と装置とが与えられる。1つの観点では、加入者識別トークンは移動体ユニットに認証支持を提供するように構成され、ここで移動体ユニットは秘密キーを介して変換用の加入者識別トークンに情報を伝達する。

【0007】

1つの観点では、無線通信システムにおいて加入者を認証するための装置が与えられ、ここで装置は無線通信システム内で動作している移動局に通信的に連結されることが可能である。この装置はメモリと、メモリ内に蓄積された1セットの命令を実施するように構成されたプロセッサとを具備し、この命令のセットは移動局から秘密を保持されるキーに基づいた一次署名(signature)と、移動局から受信される二次署名とを選択的に発生するためのものである。

10

【0008】

もう1つの観点では、加入者識別装置を使用して加入者の認証を提供するための方法が与えられる。この方法は下記の工程を具備する：複数のキーを発生する；加入者識別装置に通信的に連結された通信装置に複数のキーからの少なくとも1つのキーを送信して、この複数のキーからの少なくとも1つのキーで秘密を保持する；通信装置に送信された少なくとも1つのキーと送信メッセージとの両者を使用して通信装置で署名を発生する、ここで発生すること(generating)は少なくとも1つのキーと送信メッセージとから形成された連結値をハッシュする(hashing)ことにより実施される；加入者識別装置に署名を送信する；加入者識別装置で署名を受信する；受信された署名から一次署名を発生する、ここで発生することは少なくとも1つの秘密キーから形成された連結値と通信装置から受信された署名とをハッシュすることにより実施される；及び通信システムに一次署名を伝達する。

20

【0009】

もう1つの観点では、加入者識別モジュールが与えられる。この加入者識別モジュールはキー発生素子と、キー発生素子から秘密キーを及び移動体ユニットから情報を受信するように構成され、そして移動体ユニットに送出されるであろう署名を発生するようにさらに構成された署名発生器とを具備し、ここで署名は秘密キーを移動体ユニットからの情報と連結することにより、そして連結された秘密キー及び情報をハッシュすることにより発生される。

30

【発明を実施するための最良の形態】

【0010】

図1に図示されるように、無線通信ネットワーク10は一般に複数の移動局(加入者ユニットまたはユーザ装置とも呼ばれる)12a-12d、複数の基地局(基地局トランシーバ(BTS)またはノードBとも呼ばれる)14a-14c、基地局コントローラ(BSC)(無線ネットワーク・コントローラまたはパケット制御機能とも呼ばれる)16、移動交換局(MSC)またはスイッチ18、パケットデータ・サービング・ノード(PDSN)またはインターネットワーキング機能(IWF)20、公衆電話交換ネットワーク(PSTN)22(典型的な例では電話会社)、及びインターネット・プロトコル(IP)ネットワーク24(典型的な例ではインターネット)を含む。簡易化のために、4つの移動局12a-12d、3つの基地局14a-14c、1つのBSC16、1つのMSC18、及び1つのPDSN20が示される。いずれの数(any number)の移動局12、基地局14、BSC16、MSC18、及びPDSN20もあり得ることは、この分野の技術者により理解されるであろう。

40

【0011】

1実施形態では無線通信ネットワーク10はパケットデータ・サービス・ネットワークである。移動局12a-12dは、携帯型電話機、走行(running)IPベース、ウェブブラウザ・アプリケーションのラップトップ・コンピュータに接続されるセルラ電話機、対

50

応ハンズフリー・カーキット(associated hands-free car kits)付きのセルラ電話機、走行IPベース、ウェブブラウザー・アプリケーションの個人データ補助(PDA)、携帯型コンピュータに組み込まれた無線通信モジュール、または無線ローカル・ループやメータ読取りシステムで見つけられる可能性のある固定位置通信モジュールのような、多数の異なるタイプの無線通信装置のいずれであってもよい。最も一般的な実施形態では、移動局はいずれのタイプの通信ユニットであってもよい。

【0012】

移動局12a-12dは、例えば、EIA/TIA/IS-707標準のような、1つまたはそれ以上の無線パケットデータ・プロトコルを実行するように構成されてもよい。特定の実施形態では、移動局12a-12dはIPネットワーク24に行先を定められたIPパケットを発生して、このIPパケットをポイントツーポイント・プロトコル(PPP)を使用しているフレームにカプセル化する。

10

【0013】

1実施形態においてIPネットワーク24はPDNS20に連結され、PDNS20はMSC18に連結され、MSC18はBSC16とPSTN22とに連結され、そしてBSC16は、例えば、E1、T1、非同期転送モード(ATM)、IP、フレームリレー、HDSL、ADSL、またはxDSLを含むいくつかの既知のプロトコルのいずれかに従って音声及び/またはデータパケットの送信のために構成された有線(wirelines)を介して基地局14a-14cに連結される。代替の1実施形態では、BSC16はPDNS20に直接連結され、そしてMSC18はPDNS20には連結されない。この発明のうち1つの実施形態では、第3世代パートナーシップ・プロジェクト2“3GPP2”、“cdma2000スペクトル拡散システム用の物理層標準”、TIA/EIA/IS-2000-2-A、(草案、30版)(1999年11月19日)として公布されるように、これは引用されてこの中に完全に組み込まれており、移動局12a-12dは、3GPP2文書番号第C. P0002-A、TIA PN-4694号内に定義されたRFインターフェイスを介して基地局14a-14cと通信する。

20

【0014】

無線通信ネットワーク10の典型的な動作中、基地局14a-14cは電話呼、ウェブブラウジング(Web browsing)、または他のデータ通信において予約された種々の移動局12a-12dから複数セットの逆方向リンク信号を受信して復調する。所定の基地局14a-14cにより受信された各逆方向リンク信号はその基地局14a-14c内で処理される。各基地局14a-14cは複数セットの順方向リンク信号を変調して移動局12a-12dに送信することにより複数の移動局12a-12dと通信することができる。例えば、図1に示されるように、基地局14aは第1及び第2の移動局12a、12bと同時に通信し、そして基地局14cは第3及び第4の移動局12c、12dと同時に通信する。結果としてのパケットはBSC16に順方向送信され、それは呼資源の割当てと、基地局14a-14cの1局から基地局14a-14cの他の局への特定の移動局12a-12dのための呼のソフトハンドオフのオーケストレーション(orchestration)を含む移動性の管理機能性(management functionality)とを提供する。例えば、移動局12cは2局の基地局14b、14cと同時に通信している。結局、移動局12cが1局の基地局14cから十分遠くに離れて移動する時は、その呼は他の基地局14bにハンドオフされるであろう。

30

40

【0015】

もしも伝送が従前の(conventional)電話呼であれば、BSC16はMSC18に受信されたデータを送り、MSC18はPSTN22とのインターフェイスに対して追加のルーチングサービスを提供する。もしも伝送がIPネットワーク24を行先と定めるデータ呼のようなパケットベースの伝送であれば、MSC18はPDNS20にデータパケットを送るであろうし、PDNS20はIPネットワーク24にそのパケットを送出するであろう。代わりに、BSC16はPDNS20にそのパケットを直接送るであろうし、PDNS20はIPネットワーク24にそのパケットを送出する。

50

【0016】

図2は無線通信システム内で移動体電話機を使用している加入者を認証するための方法を図示する。彼等のホームシステム(HS)200の領域外を旅行している加入者は訪問先(visited)システム(VS)210内で移動体ユニット220を使用する。加入者は加入者識別トークンを挿入することにより移動体ユニット220を使用する。そのような加入者識別トークンは、加入者が訪問先システムで新しい口座を開設する必要無しに口座サービスにアクセスすることを可能とする、暗号及び認証情報を発生するように構成される。要求(図示された記号)は移動体ユニット220からサービスのためのVS210に送られる。VS210は加入者(図示せず)へのサービスを決定するようにHS200と連絡をとる。

10

【0017】

HS200はランダムナンバー240と加入者識別トークン上に保持された秘密情報の知識(knowledge)に基づいた予測応答(expected response)(XRES)270とを発生する。ランダムナンバー240はチャレンジ(challenge)として使用されるべきであり、ここで目標とされた(targeted)受取人は予測応答270にマッチする確認応答を発生するためにランダムナンバー240と秘密の知識とを使用する。ランダムナンバー240及びXRES270はHS200からVS210に送信される。他の情報も送信されるが、ここでは関係がない(図示せず)。HS200とVS210との間の通信は図1に記述された方法で容易にされる。VS210は移動体ユニット220にランダムナンバー240を送信して、移動体ユニット220からの確認メッセージ260の送信を待つ。確認メッセージ260とXRES270とはVS210で比較素子280で比較される。もしも確認メッセージ260とXRES270とがマッチすれば、VS210は移動体ユニット220にサービスを提供し続ける。

20

【0018】

移動体ユニット220は加入者により移動体ユニット220内に挿入された加入者識別トークン230にランダムナンバー240を送る。安全キー300は加入者識別トークン230上に蓄積される。安全キー300及びランダムナンバー240の両者は、確認メッセージ260、暗号法の暗号(cryptographic cipher)キー(CK)290、及び統合性(Integrity)キー(IK)310を発生するためにキー発生器250により使用される。CK290とIK310とは移動体ユニット220に伝達される。

30

【0019】

移動体ユニット220では、通信がそのメッセージの予定された(intended)受取人のみにより解読され得るように、CK290は移動体ユニット220とVS210との間の通信を暗号化するために使用されることができる。通信を暗号化すべく暗号キーを使用するための技術は、本発明の譲受人に譲渡され、引用されてこの中に組み込まれた、出願中の米国特許出願番号第09/143,441号、1998年8月28日提出、タイトル「暗号化ストリーム暗号を発生するための方法と装置“Method and Apparatus for Generating Encryption Stream Ciphers”」に記述されている。他の暗号化技術はこの中に記述された実施形態の範囲に影響を及ぼすこと無しに使用されることができる。

40

【0020】

IK310はメッセージ認証符号(MAC)を発生するために使用されることができ、ここでMACは送信メッセージフレームが特定の当事者から発せられたことを確かめるために、そしてそのメッセージが送信中に変更されなかったことを確かめるために、送信メッセージに付加される。MACを発生するための技術は、本発明の譲受人に譲渡され、引用されてこの中に組み込まれた、出願中の米国特許出願番号第09/371,147号、1999年8月9日提出、タイトル「メッセージ認証符号を発生するための方法と装置“Method and Apparatus for Generating a Message Authentication Code”」に記述されている。認証符号を発生するための他の技術はこの中に記述された実施形態の範囲に影響を及ぼすこと無し

50

に使用されることができる。よって、この中に使用されたような術語“署名”は、通信システムにおいて実施され得るいずれかの認証スキームの出力を表す。

【0021】

代わりに、IK310は送信メッセージと別々にまたは一緒に送信される特定の情報に基づいた認証署名340を発生するために使用されることができる。認証署名を発生するため技術は、本発明の譲受人に譲渡され、引用されてこの中に組み込まれた、米国特許番号第5,943,615号、タイトル「無線通信システムにおいて認証セキュリティを提供するための方法と装置“Method and Apparatus for Providing Authentication Security in a Wireless Communication System”」に記述されている。認証署名340はIK310を移動体ユニット220からのメッセージ350と組み合わせるハッシュ素子(hashing element)330の出力である。認証署名340とメッセージ350とは放送により(over the air)VS210に送信される。

10

【0022】

図2に見られるように、暗号化キー290と統合性キー(integrity key)310とは加入者識別トークン230から移動体ユニット220に送信され、それは放送によりパブリック・ディセミネーション(public dissemination)のためのデータフレームを発生し続ける。この技術は立ち聞きする人(eavesdropper)が放送によりそのようなキーの価値を決定するのを防ぐことができる一方で、この技術はログ・シェルによる攻撃からの保護を提供しない。ログ・シェル(rogue shell)は、CK290とIK310とを受け入れるように、そしてその後そのようなキーの存在をローカルメモリから一掃する(purging)よりはむしろそのキーを蓄積するようにプログラムされることができる。キーを盗むもう1つの方法は、移動体ユニット220が他の位置への受信キーを送信するようにプログラムすることである。CK290とIK310とはその後、加入者に権限のない通信を不正に広告する(bill)ために使用されることができる。ホームシステム200で発生されたランダムナンバーは、同様の発生されたキーが拡大期間の間中使用される場合のように、不安定な方法で(in a manner that is insecure)使用されるシステムにおいて、このログ・シェル攻撃は特に有効である。

20

【0023】

ログ・シェル攻撃に備えて保護する1実施形態は、加入者識別トークンの挿入無しには移動体ユニットにより再生され得ない電子署名を発生するために、プロセッサと加入者識別トークン内のメモリとを使用する。

30

【0024】

図3は無線通信システムにおいて加入者のローカル認証を実行するための1実施形態を図示する。この実施形態では、加入者識別トークン230は移動体ユニット220に渡されないキーに基づいた認証応答を発生するようにプログラムされる。よって、もしも加入者により使用された移動体ユニットがログ・シェルであれば、そのログ・シェルは適正な認証応答を再現することはできない。

【0025】

図2に記述された方法と同様に、移動体ユニット220は加入者識別トークン230から受信されるIK310とVS210に送られるべきメッセージとに基づいた署名信号を発生する。しかしながら、1実施形態では、署名信号はVSには渡されない。署名信号は加入者識別トークン230に渡されて、一次署名信号を発生するために付加キーと一緒に使用される。一次署名信号は移動体ユニット220に送出され、それは認証のためのVS210に一次署名信号を順番に送信する。

40

【0026】

HS200はランダムナンバー240と加入者識別トークン上に保持された安全キーの知識に基づいた予測応答(XRES)270とを発生する。ランダムナンバー240とXRES270とはVS210に送信される。HS200とVS210との間の通信は図1に記述された方法で容易にされる。VS210は移動体ユニット220にランダムナンバー

50

240を送信して、移動体ユニット220から確認メッセージ260の送信を待つ。確認メッセージ260とXRES270とはVS210での比較素子280で比較される。もしも確認メッセージ260とXRES270とがマッチすれば、VS210は移動体ユニット220にサービスを提供し続ける。

【0027】

移動体ユニット220は加入者により移動体ユニット220と電子的に連結された加入者識別トークン230にランダムナンバー240を伝達する。安全キー300は加入者識別トークン230上に蓄積される。安全キー300とランダムナンバー240との両者は確認メッセージ260、暗号キー（CK）290、統合性キー（IK）310、及びUIM認証キー（UAK）320を発生するためにキー発生器250により使用される。CK290とIK310とは移動体ユニット220に伝達される。

10

【0028】

移動体ユニット220で、CK290は送信データフレーム（図3に図示せず）を暗号化するために使用される。IK310は署名信号340を発生するために使用される。署名信号340はIK310と移動体ユニット220からのメッセージ350上に、ハッシュ機能のような、暗号化演算(encryption operation)または片方向演算(one-way operation)を行使する署名発生器330の出力である。署名信号340は加入者識別トークン230に送信される。加入者識別トークン230で、署名信号340とUAK320とは一次署名信号370を発生するために署名発生器360により処理される。一次署名信号370は移動体ユニット220に、そしてVS210に送信され、そこでは検証素子380は加入者のアイデンティティを認証する。検証素子380は署名信号340と一次署名信号370とを再生することにより検証を達成することができる。代わりに、検証素子380は移動体ユニット220から署名信号340を受信することができ、一次署名信号370のみを再生する。

20

【0029】

署名信号340及びVS210での一次署名信号370の再生は、いろいろな技術により達成され得る。1実施形態では、検証素子380はホームシステム200からのUAK390及び統合性キーを受信できる。検証素子380はまた移動体ユニット220からメッセージ350を受信すると、署名信号が発生されて、その後一次署名要素を発生するために使用されることができる。

30

【0030】

加入者識別トークン230内の署名発生器360はメモリとプロセッサとを備えることができる。ここでプロセッサはいろいろな技術を使用して入力処理するように構成されることが可能である。これらの技術は暗号化技術、ハッシュ機能、または非可逆動作の形式を取ることができる。1例として、加入者識別トークンにより実施され得る1技術は、1994年5月、連邦情報処理標準(FIPS) PUB186、“デジタル署名標準(Digital Signature Standard)”において公布された、安全ハッシュアルゴリズム(SHA)である。加入者識別トークンにより実行され得るもう1つの技術は、1977年1月、FIPS PUB46において公布された、データ暗号化標準(DES)である。この中で使用されたように、術語“暗号化”の使用は必ずしも動作が可逆的で無ければならないことを意味しない。ここに記述された実施形態では、動作は非可逆的であってもよい。

40

【0031】

キー発生器250もまたメモリとプロセッサとを備えることができる。実際に、1実施形態では、単一のプロセッサが署名発生器360とキー発生器250との機能を達成するように構成されることができる。検証は検証素子380で同じ入力から同じ結果を計算して、計算された値と送信された値とを比較することにより実行されることができる。

【0032】

上記実施形態のより詳細な記述では、信号発生器330はこの中にHMAC-SHA-1として引用された技術を実施するように構成されることができる。上述の実施形態では、

50

ハッシュ機能は署名信号340を発生するために信号発生器330内で使用され得ることが注目された。ハッシュベースのMACs (HMACs)の説明は、論文“メッセージ認証のためのキーイングハッシュ機能 (Keying Hash Functions for Message Authentication)”、ベラレ等、暗号作成術 (Cryptography)における進歩—暗号 (Crypto) 96 議事録、コンピュータ・サイエンス1109巻、スプリングーヴァーラグ、1996年における講義ノート、内に見つけることができる。HMACは、2ステップ処理において、SHA-1のような、暗号化ハッシュ機能を使用するMACスキームである。HMAC-SHA-1スキームでは、ランダム及び秘密キーはSHA-1機能を初期化し、それはその後メッセージの1ダイジェストを生成する (produce) ために使用される。このキーはその後第1のダイジェストの1ダイジェストを生成するようにSHA-1を再び初期化するために使用される。この第2のダイジェストは各メッセージに付加されるであろうMACを提供する。この中に記述された実施形態では、加入者識別トークン230により発生される統合性キー (IK)は、SHA-1を初期化しているランダム及び秘密キーとして使用されることが出来る。図4は、加入者識別トークンからの統合性キーにより初期化される移動局内のHMACの実施の形態と、UIM認証キーにより初期化される加入者識別トークン内のHMACの実施の形態とを図示する図である。

10

【0033】

図4において、HS200はランダムナンバー240と加入者識別トークン230上に保持された秘密情報の知識に基づいた予測応答 (XRES) 270とを発生する。ランダムナンバー240とXRES270とはVS210に送信される。HS200とVS210との間の通信は図1に記述された方法で容易にされる。VS210は移動体ユニット220にランダムナンバー240を送信して、移動体ユニット220からの確認メッセージ260の送信を待つ。確認メッセージ260とXRES270とはVS210での比較素子280で比較される。もしも確認メッセージ260とXRES270とがマッチすれば、VS210は移動体ユニット220にサービスを提供し続ける。

20

【0034】

移動体ユニット220は、加入者により移動体ユニット220と電子的に連結された加入者識別トークン230にランダムナンバー240を伝達する。安全キー300は加入者識別トークン230上に蓄積される。安全キー300とランダムナンバー240との両者は、確認メッセージ260、暗号化キー (CK) 290、統合性キー (IK) 310、及びUIM認証キー (UAK) 320を発生するためにキー発生器250により使用される。CK290とIK310とは移動体ユニット220に伝達される。

30

【0035】

移動体ユニット220では、CK290は送信データフレーム (図4には図示せず)を暗号化するために使用される。IK310は署名発生器330から署名信号340を発生するために使用される。署名発生器330はSHA-1の使用によってメッセージ260の変換を生成するように構成される。SHA-1ハッシュ機能はIK310により初期化される。

【0036】

メッセージ260を変換するSHA-1ハッシュ機能の結果である署名信号340は、加入者識別トークン230に送信される。加入者識別トークン230で、署名信号340とUAK320とは、署名発生器360により処理され、UIMメッセージ認証符号 (UMAC) 370である署名信号340の変換を生成する (generate)。署名発生器360もまたSHA-1ハッシュ機能を実施するように構成される。しかしながら、この機能はその後IK310よりはむしろUAK320を使用して初期化される。

40

【0037】

UMAC370は移動体ユニット220とVS210とに送信され、そこで検証素子380は加入者のアイデンティティを認証する。検証素子380は署名信号340とUMAC370とを再生することにより検証を達成する。代わりに、検証素子380は移動体ユニ

50

ット 2 2 0 から署名信号 3 4 0 を受信して、U M A C 3 7 0 のみを再生することができる。

【 0 0 3 8 】

図 5 は実施形態の一般化された説明を図示するフローチャートである。ステップ 5 0 0 で、移動体ユニットは認証を要求するメッセージを発生する。ステップ 5 0 1 で、移動体ユニットは加入者識別トークンから長さ L の統合性キー (I K) を受信する。ステップ 5 0 2 で、移動体ユニットは統合性キー I K を長さ b、ここで b は移動体ユニット内部の署名発生器のハッシュ機能のブロックサイズである、にパッドする (pads)。1 実施形態では、キーは長さ b にゼロパッドされる (zero-padded) ことができる。他の実施形態では、キーは長さ b のパディング定数と X O R される。もしも I K が既に長さ b を有するならば、そのときはこのステップは省略されることができる。ステップ 5 0 4 で、パッドされた I K は認証を必要とするメッセージと連結される。パッドされた I K とメッセージとの連結はその後、S H A のようなハッシュ機能を実施するように構成された署名発生器によりステップ 5 0 5 で細分される。1 実施形態では、X O R 動作の出力はメモリ素子内に保存され、そしてもしも加入者識別トークンからの I K がその通信セッションの間中同一の物のままならば、さらなる使用に対して (for further use) 取り消される (recalled) ことができる。

10

【 0 0 3 9 】

もしも U I M 認証キー (U A K) が使用されるようであれば、その後プログラムフローはステップ 5 1 0 に進む。もしも U A K が使用されないようであれば、その後プログラムフローはステップ 5 2 0 に進む。

20

【 0 0 4 0 】

ステップ 5 1 0 で、ステップ 5 0 5 からの細分されたメッセージは加入者識別トークンに送信される。ステップ 5 1 1 で、U A K が既に長さ b でなければ、加入者識別トークンは U A K を長さ b にパッドする。パッドされた I K は、次のメッセージが通信セッションの間に認証を必要とする時に、再使用のためのメモリに蓄積されることができる。ステップ 5 1 2 で、パッドされた I K と細分されたメッセージとは連結されて、署名発生器に入力される。署名発生器は、ステップ 5 1 3 で S H A - 1 のような、ハッシュ機能を実施するように構成される。ステップ 5 1 4 で、署名発生器の出力は加入者識別トークンから移動体ユニットに送信される。

30

【 0 0 4 1 】

ステップ 5 2 0 で、同じ統合性キーは既に細分されたメッセージを再細分する (rehash) ために使用される。ステップ 5 0 5 からの細分されたメッセージは移動体ユニット内部の第 2 の署名発生器に送られる。あるいは代わりに、細分されたメッセージはステップ 5 0 5 の署名発生器に再挿入されてもよい。もしも 1 個の統合性キーが 2 つのハッシュ処理において使用されるようであれば、その時この統合性キーはハッシュ発生器の各々が異なる値で初期化されるように変更されねばならない。例えば、各ハッシュステップについて、統合性キーは両方とも長さが b の、定数値 c_1 または定数値 c_2 のいずれかにビットワイズ (bit-wise) を付加されることができる。この方法を使用して、1 つの統合性キーのみが加入者識別トークンにより発生されることが必要である。

40

【 0 0 4 2 】

より安全な実施形態は第 2 のハッシュステップが加入者識別トークンで U A K を使用して実行される実施の形態であることは注目されねばならない。

【 0 0 4 3 】

図 5 に記述された処理は下記の式により数学的に記述されることができる：

$$H M A C (x) = F_{token} (U A K , F_{mobile} (I K , x))$$

ここで $F_Y ()$ は位置 Y で実行されたハッシュ関数を表し、x は原メッセージを表し、U A K 及び I K はキーであり、そしてコンマは連結を表す。

【 0 0 4 4 】

C D M A システムまたは G S M システムにおいて使用され、また R - U I M または U S I

50

Mとしても知られる加入者識別トークンは、それぞれ、上述された方法における一次署名信号またはU M A Cを発生するように構成されることができ、すなわち、移動体ユニットにより発生された全メッセージは暗号化されて、認証される。しかしながら、そのようなトークン内の中央処理ユニットは限定され得るので、代替の実施形態を実施することが望ましいかも知れず、ここで重要性の重みは、重要なメッセージのみが安全に暗号化されて認証されるようにメッセージフレームに割り当てられる。例えば、ビリング情報を含むメッセージフレームは、ボイス・パイロードを含むメッセージフレームよりも、増加された安全性について、より多くの必要性を有する。よって、移動体ユニットはビリング情報メッセージフレームに重要性のより大きい重みを割り当て、またボイス・メッセージフレームに重要性のより小さい重みを割り当てることができる。加入者識別トークンがこれらの重み付けされたメッセージから発生された署名信号を受信すると、C P Uは各署名信号に付加された重要性の種々の重みを査定する(assess)ことができ、そして重く重み付けされた署名信号に対してのみ一次署名信号を決定することができる。代わりに、移動体ユニットは加入者識別トークンに“重要な”署名信号のみを伝達するようにプログラムされることができる。選択的一次署名信号発生はこの方法は、加入者識別トークンの処理負荷を軽減することにより加入者識別トークンの効率を増加させる。

10

【0045】

上述された実施形態は、加入者識別トークンと移動体ユニットとの間のより安全な処置(transaction)を要求することにより、加入者の口座の権限のない使用を防ぐ。移動体ユニットは秘密のU A Kの知識無しには一次署名信号を発生できないので、ログ・シェルとして活動するようにプログラムされる移動体ユニットは、違法な目的のために加入者情報を乱用する(misappropriate)ことはできない。

20

【0046】

上述された実施形態はまた、メッセージよりはむしろ、署名信号上で動作することにより加入者識別トークンの処理能力を最大にする。典型的に、署名信号はメッセージよりもより短いビット長を有するであろう。よって、送信メッセージフレームよりはむしろ署名信号上で動作するために、加入者識別における署名発生器として、より少ない時間が必要となる。上記されたように、加入者識別トークンの処理能力は通常、移動体ユニットの処理能力よりもずっと小さい。よって、この実施形態の実施は、スピードを犠牲にすること無しにメッセージの安全な認証を提供するであろう。

30

【0047】

しかしながら、プロセッサ構造における改良がほとんど指数関数的なペースで発生することは注目されねばならない。そのような改良はより速い処理時間と、より小さいプロセッサ・サイズとから成る。よって、ローカル認証を提供するもう1つの実施形態が実施されることができ、そこでは一次署名信号は短い署名信号を介して間接よりはむしろ、1メッセージから直接発生されることができる。移動体ユニットは、移動体ユニット内部の署名発生素子にメッセージを渡すよりはむしろ、一次署名信号をすぐに発生する能力を有するもの、加入者識別トークンにメッセージを直接渡すように構成されることができる。もう1つの実施形態では、前記メッセージのために必要とされる安全度に従って、限られた数のメッセージのみが加入者識別ユニットに直接渡される必要がある。

40

【0048】

種々の実施形態が無線通信システムの文脈内に記述されたが、一方で、種々の実施形態が、通信ネットワーク内に接続されたよく知られていない端末を使用しているいずれの当事者にも安全なローカル認証を提供するために、さらに使用され得ることは注目されねばならない。

【0049】

このように、通信システムにおいて加入者のローカル認証を実行するための新規な及び改良された方法及び装置が記述された。この分野の技術者は、この中に開示された実施形態に関して記述された種々の実例となる論理ブロック、モジュール、回路、及びアルゴリズム・ステップは電子ハードウェア、ソフトウェア、ファームウェア、またはその組合わ

50

せとして実施されてもよいことを理解するであろう。種々の事例となる構成要素、ブロック、モジュール、回路、及びステップは、一般にそれらの機能性の表現で記述された。機能性がハードウェア、ソフトウェア、またはファームウェアとして実施されるかどうかはシステム全体に課された特定のアプリケーションと設計の制約とによる。これらの環境下でのハードウェア、ソフトウェア、及びファームウェアの互換性、及び各特定のアプリケーションについて記述された機能性を実施することがいかにベストであるかを、熟練技工は認める。

【0050】

種々の事例となる論理ブロック、モジュール、回路、及びこの中に開示された実施形態に関して記述されたアルゴリズム・ステップは、デジタル信号プロセッサ（DSP）、特定用途向け集積回路（ASIC）、フィールド・プログラム可能なゲートアレイ（FPGA）または他のプログラム可能な論理装置、ディスクリート・ゲートカトランジスタ論理、ディスクリート・ハードウェア構成要素で実施または実行されることができ。1セットのファームウェア命令を実行するプロセッサ、いずれか従前のプログラム可能なソフトウェア・モジュールとプロセッサ、またはそのいずれかの組み合わせは、この中に記述された機能を実行するように設計されることが可能である。プロセッサは好都合にマイクロプロセッサであってもよいが、しかし代替案では、プロセッサはいずれか従前のプロセッサ、コントローラ、マイクロコントローラ、またはステートマシンであってもよい。ソフトウェア・モジュールはRAMメモリ、フラッシュ・メモリ、ROMメモリ、EPROMメモリ、EEPROMメモリ、レジスタ、ハードディスク、着脱可能形ディスク、CD-ROM、あるいはこの分野において既知のいずれか他の形式の蓄積媒体に属することができる。例示的なプロセッサは蓄積媒体から情報を読み取り、そしてそれに情報を書き込むように蓄積媒体に連結される。代替案では、蓄積媒体はASIC内に存ってもよい。ASICは電話機または他のユーザ端末内に存ってもよい。代替案では、プロセッサと蓄積媒体とは電話機または他のユーザ端末内に存ってもよい。プロセッサはDSPとマイクロプロセッサとの組み合わせとして、またはDSPコアなどとともに2台のマイクロプロセッサとして実施されてもよい。技術者は上記説明の全体を通して参照されることができデータ、指示、命令、情報、信号、ビット、記号、及びチップが、電圧、電流、電磁波、磁界または粒子、光学界または粒子、あるいはそのいずれかの組み合わせにより表されることをさらに認めるであろう。

【0051】

本発明の種々の実施形態はこのように示され、そして記述された。しかしながら、この分野における正規の技術の1つにとって、この発明の精神または範囲を逸脱すること無しにここに開示された実施形態に多くの変更がなされてもよいことは明白であろう。

【図面の簡単な説明】

【0052】

【図1】典型的なデータ通信システムを示す図。

【図2】本発明の無線通信システム内の構成要素間の通信交換を示す図。

【図3】本発明の加入者識別トークンが移動体ユニットに暗号支持(encryption support)を提供する1実施形態を示す図。

【図4】本発明のハッシュ機能が認証署名を発生するために使用される1実施形態を示す図。

【図5】本発明の認証署名を発生するためにメッセージをハッシュするための1方法を示すフローチャート。

【符号の説明】

【0053】

12a-12d…MS、14a-14c…BTS、16…BSC、18…MSC、20…PDN、22…PSTN、24…IPネットワーク、200…ホームシステム、210…訪問先システム、220…移動体ユニット、230…加入者識別トークン、240…ランダムナンバー、250…キー発生器、260…RES、270…XRES、280…比

10

20

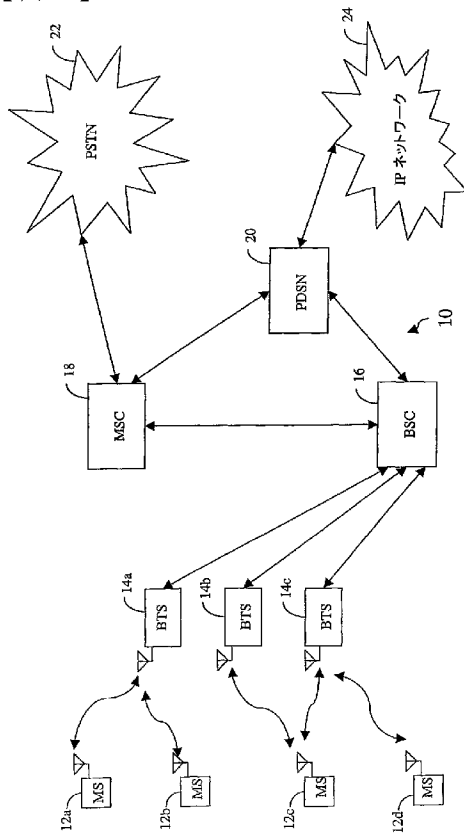
30

40

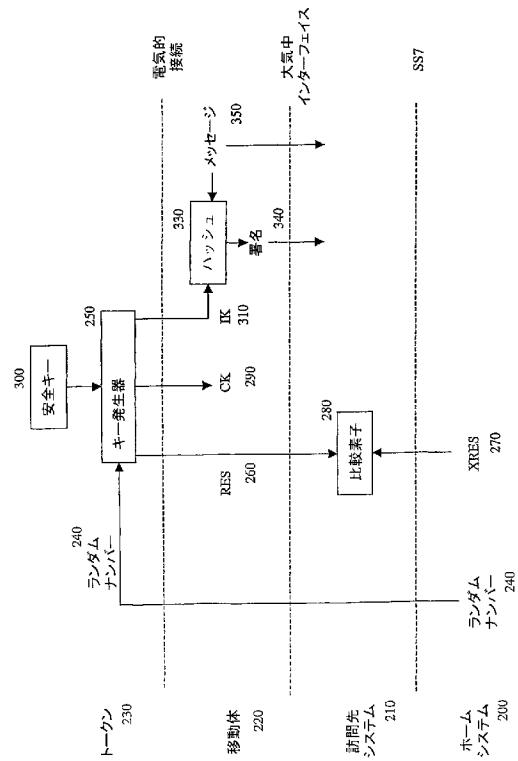
50

較素子、290…CK、300…安全キー、310…IK、320…UAK、330…ハッシュ機能、340…署名、350…メッセージ、360…署名発生器、370…一次署名、380…検証素子、390…UAK及びIK

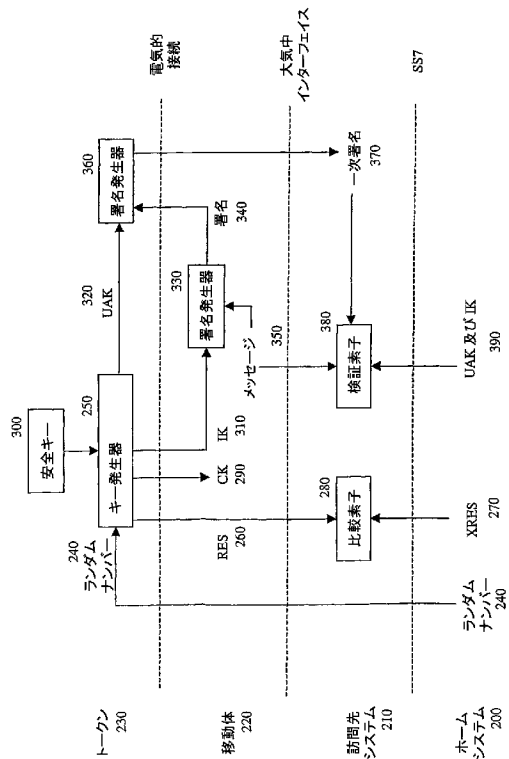
【図1】



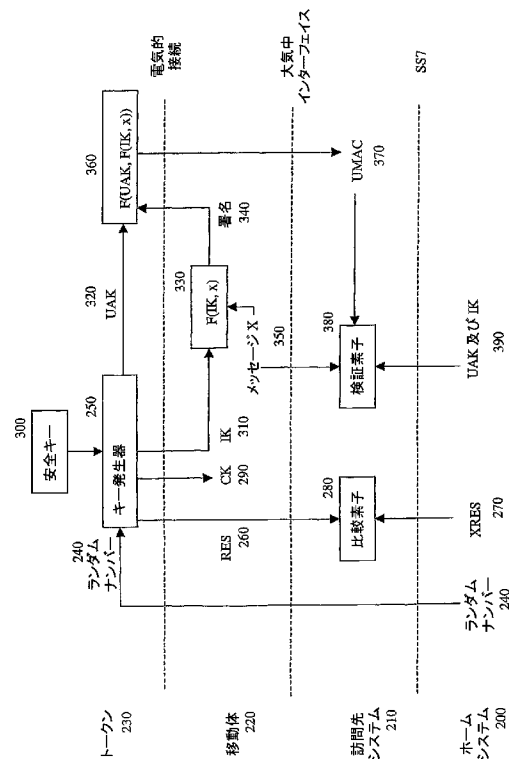
【図2】



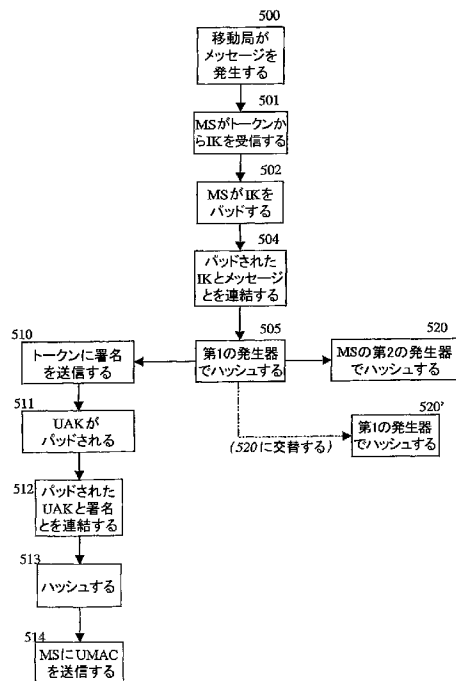
【図3】



【図4】



【図5】



【国際公開パンフレット】

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau(43) International Publication Date
28 November 2002 (28.11.2002)

PCT

(10) International Publication Number
WO 02/096150 A1(51) International Patent Classification: H04Q 7/38
H04L 9/32, 29/06, H04Q 7/32

(74) Agents: WADSWORTH, Philip, R. et al.; Qualcomm Incorporated, 5775 Morehouse Drive, San Diego, CA 92121-1714 (US).

(21) International Application Number: PCT/US02/16103

(22) International Filing Date: 21 May 2002 (21.05.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data: 09/863,139 22 May 2001 (22.05.2001) US

(71) Applicant: QUALCOMM INCORPORATED (US/US); 5775 Morehouse Drive, San Diego, CA 92121-1714 (US).

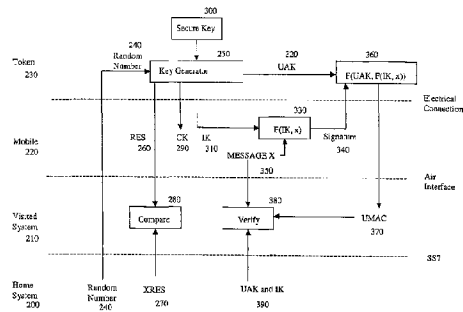
(72) Inventors: QUICK, Roy, E., Jr.; 1150 Barcelona Drive, San Diego, CA 92107 (US); ROSE, Gregory, G.; 6 Kingston Avenue, Morfela, NSW 2157 (AU).

(81) Designated States (national): AF, AG, AI, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GL, GR, GM, HR, HU, ID, IL, IN, IS, JP, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MY, NZ, OM, PA, PE, PG, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZM, ZW.

(84) Designated States (regional): ARIPO patent (GL, GM, KE, LS, MW, MZ, SD, SI, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CI, CG, CF, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: LOCAL AUTHENTICATION IN A COMMUNICATION SYSTEM



(57) Abstract: Methods and apparatus are presented for providing local authentication of subscribers travelling outside their home systems. A subscriber identification token (230) provides authentication support by generating a signature (370) based upon a key that is held secret from a mobile unit (220). A mobile unit (220) that is programmed to wrongfully retain keys from a subscriber identification token (230) after a subscriber has removed his or her token is prevented from subsequently accessing the subscriber's account.

WO 02/096150 A1

WO 02/096150 A1 **Published:**

— with international search report

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

WO 02/096150

PCT/US02/16103

1

LOCAL AUTHENTICATION IN A COMMUNICATION SYSTEM

BACKGROUND

5

I. Field of the Invention

The present invention relates to communication systems, and more particularly, to local authentication of a communication system subscriber.

10 II. Background

The field of wireless communications has many applications including, e.g., cordless telephones, paging, wireless local loops, personal digital assistants (PDAs), Internet telephony, and satellite communication systems. A particularly important application is cellular telephone systems for mobile subscribers. As used herein, the term "cellular" system encompasses both cellular and personal communications services (PCS) frequencies. Various over-the-air interfaces have been developed for such cellular telephone systems including, e.g., frequency division multiple access (FDMA), time division multiple access (TDMA), and code division multiple access (CDMA). In connection therewith, various domestic and international standards have been established including, e.g., Advanced Mobile Phone Service (AMPS), Global System for Mobile (GSM), and Interim Standard 95 (IS-95). In particular, IS-95 and its derivatives, IS-95A, IS-95B, ANSI J-STD-008 (often referred to collectively herein as IS-95), and proposed high-data-rate systems for data, etc. are promulgated by the Telecommunication Industry Association (TIA) and other well known standards bodies.

Cellular telephone systems configured in accordance with the use of the IS-95 standard employ CDMA signal processing techniques to provide highly efficient and robust cellular telephone service. Exemplary cellular telephone systems configured substantially in accordance with the use of the IS-95 standard are described in U.S. Patent Nos. 5,103,459 and 4,901,307, which are assigned to the assignee of the present invention and incorporated

30

WO 02/096150

PCT/US02/16103

2

by reference herein. An exemplary system utilizing CDMA techniques is the cdma2000 ITU-R Radio Transmission Technology (RTT) Candidate Submission (referred to herein as cdma2000), issued by the TIA. The standard for cdma2000 is given in the draft versions of IS-2000 and has been
5 approved by the TIA. The cdma2000 proposal is compatible with IS-95 systems in many ways. Another CDMA standard is the W-CDMA standard, as embodied in 3rd Generation Partnership Project "3GPP", Document Nos. 3G TS 25.211, 3G TS 25.212, 3G TS 25.213, and 3G TS 25.214.

Given the ubiquitous proliferation of telecommunications services in
10 most parts of the world and the increased mobility of the general populace, it is desirable to provide communication services to a subscriber while he or she is travelling outside the range of the subscriber's home system. One method of satisfying this need is the use of an identification token, such as the Subscriber Identity Module (SIM) in GSM systems, wherein a subscriber is
15 assigned a SIM card that can be inserted into a GSM phone. The SIM card carries information that is used to identify the billing information of the party inserting the SIM card into a mobile phone. Next generation SIM cards have been renamed as USIM (UTMS SIM) cards. In a CDMA system, the identification token is referred to as a Removable User Interface Module (R-
20 UIM) and accomplishes the same purpose. Use of such an identification token allows a subscriber to travel without his or her personal mobile phone, which may be configured to operate on frequencies that are not used in the visited environment, and to use a locally available mobile phone without incurring costs in establishing a new account.

Although convenient, the use of such identification tokens to access
25 account information of a subscriber can be insecure. Currently, such identification tokens are programmed to transmit private information, such as a cryptographic key used for message encryption or an authentication key for identifying the subscriber, to the mobile phone. A person contemplating the
30 theft of account information can accomplish his or her goal by programming a mobile phone to retain private information after the identification token has been removed, or to transmit the private information to another storage unit

WO 02/096150

PCT/US02/16103

3

during the legitimate use of the mobile phone. Mobile phones that have been tampered in this manner will hereafter be referred to as "rogue shells." Hence, there is a current need to preserve the security of the private information stored on an identification token while still facilitating the use of said private information to access communication services.

Summary

A novel method and apparatus for providing secure authentication to a subscriber roaming outside his or her home system are presented. In one aspect, a subscriber identification token is configured to provide authentication support to a mobile unit, wherein the mobile unit conveys information to the subscriber identification token for transformation via a secret key.

In one aspect, an apparatus for authenticating a subscriber in a wireless communication system is presented, wherein the apparatus can be communicatively coupled to a mobile station operating within the wireless communications system. The apparatus comprises a memory and a processor configured to implement a set of instructions stored in the memory, the set of instructions for selectively generating a primary signature based upon a key that is held private from the mobile station and a secondary signature that is received from the mobile station.

In another aspect, a method for providing authentication of a subscriber using a subscriber identification device is presented. The method comprises the steps of: generating a plurality of keys; transmitting at least one key from the plurality of keys to a communications device communicatively coupled to the subscriber identification device and holding private at least one key from the plurality of keys; generating a signature at the communications device using both the at least one key transmitted to the communications device and a transmission message, wherein generating is implemented by hashing a concatenated value formed from the at least one key and the transmission message; transmitting the signature to the subscriber identification device; receiving the signature at the subscriber identification device; generating a

WO 02/096150

PCT/US02/16103

4

primary signature from the received signature, wherein the generating is implemented by hashing a concatenated value formed from the at least one private key and the signature received from the communications device; and conveying the primary signature to a communications system.

- 5 In another aspect, a subscriber identification module is presented. The subscriber identification module comprises a key generation element and a signature generator configured to receive a secret key from the key generation element and information from a mobile unit, and further configured to generate a signature that will be sent to the mobile unit, wherein the
10 signature is generated by concatenating the secret key with the information from the mobile unit and hashing the concatenated secret key and information.

Detailed Description of the Drawings

- 15 FIG. 1 is a diagram of an exemplary data communication system.
FIG. 2 is a diagram of a communication exchange between components in a wireless communication system.
FIG. 3 is a diagram of an embodiment wherein a subscriber identification token provides encryption support to a mobile unit.
20 FIG. 4 is a diagram of an embodiment wherein a hashing function is used to generate an authentication signature.
FIG. 5 is a flow chart of a method to hash a message in order to generate an authentication signature.

Detailed Description of the Embodiments

- 25 As illustrated in FIG. 1, a wireless communication network 10 generally includes a plurality of mobile stations (also called subscriber units or user equipment) 12a-12d, a plurality of base stations (also called base station transceivers (BTSs) or Node B) 14a-14c, a base station controller (BSC) (also
30 called radio network controller or packet control function 16), a mobile switching center (MSC) or switch 18, a packet data serving node (PDSN) or interworking function (IWF) 20, a public switched telephone network

WO 02/096150

PCT/US02/16103

5

(PSTN) 22 (typically a telephone company), and an Internet Protocol (IP) network 24 (typically the Internet). For purposes of simplicity, four mobile stations 12a-12d, three base stations 14a-14c, one BSC 16, one MSC 18, and one PDSN 20 are shown. It would be understood by those skilled in the art that there could be any number of mobile stations 12, base stations 14, BSCs 16, MSCs 18, and PDSNs 20.

In one embodiment the wireless communication network 10 is a packet data services network. The mobile stations 12a-12d may be any of a number of different types of wireless communication device such as a portable phone, a cellular telephone that is connected to a laptop computer running IP-based, Web-browser applications, a cellular telephone with associated hands-free car kits, a personal data assistant (PDA) running IP-based, Web-browser applications, a wireless communication module incorporated into a portable computer, or a fixed location communication module such as might be found in a wireless local loop or meter reading system. In the most general embodiment, mobile stations may be any type of communication unit.

The mobile stations 12a-12d may be configured to perform one or more wireless packet data protocols such as, for example, the EIA/TIA/IS-707 standard. In a particular embodiment, the mobile stations 12a-12d generate IP packets destined for the IP network 24 and encapsulate the IP packets into frames using a point-to-point protocol (PPP).

In one embodiment the IP network 24 is coupled to the PDSN 20, the PDSN 20 is coupled to the MSC 18, the MSC 18 is coupled to the BSC 16 and the PSTN 22, and the BSC 16 is coupled to the base stations 14a-14c via wirelines configured for transmission of voice and/or data packets in accordance with any of several known protocols including, e.g., E1, T1, Asynchronous Transfer Mode (ATM), IP, Frame Relay, HDSL, ADSL, or xDSL. In an alternate embodiment, the BSC 16 is coupled directly to the PDSN 20, and the MSC 18 is not coupled to the PDSN 20. In another embodiment of the invention, the mobile stations 12a-12d communicate with the base stations 14a-14c over an RIF interface defined in the 3rd Generation Partnership Project 2 "3GPP2", "Physical Layer Standard for cdma2000

WO 02/096150

PCT/US02/16103

6

Spread Spectrum Systems," 3GPP2 Document No. C.P0002-A, TIA PN-4694, to be published as TIA/EIA/IS-2000-2-A, (Draft, edit version 30) (Nov. 19, 1999), which is fully incorporated herein by reference.

During typical operation of the wireless communication network 10, the
5 base stations 14a-14c receive and demodulate sets of reverse-link signals from various mobile stations 12a-12d engaged in telephone calls, Web browsing, or other data communications. Each reverse-link signal received by a given base station 14a-14c is processed within that base station 14a-14c. Each base station 14a-14c may communicate with a plurality of mobile
10 stations 12a-12d by modulating and transmitting sets of forward-link signals to the mobile stations 12a-12d. For example, as shown in FIG. 1, the base station 14a communicates with first and second mobile stations 12a, 12b simultaneously, and the base station 14c communicates with third and fourth mobile stations 12c, 12d simultaneously. The resulting packets are forwarded
15 to the BSC 16, which provides call resource allocation and mobility management functionality including the orchestration of soft handoffs of a call for a particular mobile station 12a-12d from one base station 14a-14c to another base station 14a-14c. For example, a mobile station 12c is communicating with two base stations 14b, 14c simultaneously. Eventually,
20 when the mobile station 12c moves far enough away from one of the base stations 14c, the call will be handed off to the other base station 14b.

If the transmission is a conventional telephone call, the BSC 16 will route the received data to the MSC 18, which provides additional routing services for interface with the PSTN 22. If the transmission is a packet-based
25 transmission such as a data call destined for the IP network 24, the MSC 18 will route the data packets to the PDSN 20, which will send the packets to the IP network 24. Alternatively, the BSC 16 will route the packets directly to the PDSN 20, which sends the packets to the IP network 24.

FIG. 2 illustrates a method for authenticating a subscriber using a
30 mobile phone in a wireless communication system. A subscriber travelling outside of the range of his or her Home System (HS) 200 uses a mobile unit 220 in a Visited System (VS) 210. The subscriber uses the mobile unit 220 by

WO 02/096150

PCT/US02/16103

7

inserting a subscriber identification token. Such a subscriber identification token is configured to generate cryptographic and authentication information that allows a subscriber to access account services without the need for establishing a new account with the visited system. A request (note shown in figure) is sent from the mobile unit 220 to the VS 210 for service. VS 210 contacts HS 200 to determine service to the subscriber (not shown in figure).

HS 200 generates a random number 240 and an expected response (XRES) 270 based on knowledge of the private information held on the subscriber identification token. The random number 240 is to be used as a challenge, wherein the targeted recipient uses the random number 240 and private knowledge to generate a confirmation response that matches the expected response 270. The random number 240 and the XRES 270 are transmitted from the HS 200 to the VS 210. Other information is also transmitted, but is not relevant herein (not shown in figure). Communication between the HS 200 and the VS 210 is facilitated in the manner described in Fig. 1. The VS 210 transmits the random number 240 to the mobile unit 220 and awaits the transmission of a confirmation message 260 from the mobile unit 220. The confirmation message 260 and the XRES 270 are compared at a compare element 280 at the VS 210. If the confirmation message 260 and XRES 270 match, the VS 210 proceeds to provide service to the mobile unit 220.

Mobile unit 220 sends the random number 240 to the subscriber identification token 230 that has been inserted inside the mobile unit 220 by the subscriber. A Secure Key 300 is stored on the subscriber identification token 230. Both the Secure Key 300 and the random number 240 are used by a key generator 250 to generate the confirmation message 260, a cryptographic Cipher Key (CK) 290, and an Integrity Key (IK) 310. The CK 290 and IK 310 are conveyed to the mobile unit 220.

At the mobile unit 220, the CK 290 can be used to encrypt communications between the mobile unit 220 and the VS 210, so that communications can be decrypted only by the intended recipient of the message. Techniques for using a cryptographic key to encrypt

WO 02/096150

PCT/US02/16103

8

communications are described in co-pending U.S. Patent Application 09/143,441, filed on August 28, 1998, entitled, "Method and Apparatus for Generating Encryption Stream Ciphers," assigned to the assignee of the present invention, and incorporated by reference herein. Other encryption techniques can be used without affecting the scope of the embodiments described herein.

The IK 310 can be used to generate a message authentication code (MAC), wherein the MAC is appended to a transmission message frame in order to verify that the transmission message frame originated from a particular party and to verify that the message was not altered during transmission. Techniques for generating MACs are described in co-pending U.S. Patent Application No. 09/371,147, filed on August 9, 1999, entitled, "Method and Apparatus for Generating a Message Authentication Code," assigned to the assignee of the present invention and incorporated by reference herein. Other techniques for generating authentication codes may be used without affecting the scope of the embodiments described herein. Hence, the term "signature" as used herein represents the output of any authentication scheme that can be implemented in a communication system.

Alternatively, the IK 310 can be used to generate an authentication signature 340 based on particular information that is transmitted separately or together with the transmission message. Techniques for generating an authentication signature are described in U.S. Patent 5,943,615, entitled, "Method and Apparatus for Providing Authentication Security in a Wireless Communication System," assigned to the assignee of the present invention and incorporated by reference herein. The authentication signature 340 is the output of a hashing element 330 that combines the IK 310 with a message 350 from the mobile unit 220. The authentication signature 340 and the message 350 are transmitted over the air to the VS 210.

As seen in FIG. 2, the cryptographic key 290 and the integrity key 310 are transmitted from the subscriber identification token 230 to the mobile unit 220, which proceeds to generate data frames for public dissemination over the air. While this technique may prevent an eavesdropper from determining

WO 02/096150

PCT/US02/16103

9

the values of such keys over the air, this technique does not provide protection from attack by a rogue shell. A rogue shell can be programmed to accept the CK 290 and the IK 310, and to then store the keys rather than purging the presence of such keys from local memory. Another method to steal keys is to program the mobile unit 220 to transmit received keys to another location. The CK 290 and the IK 310 can then be used to fraudulently bill unauthorized communications to the subscriber. This rogue shell attack is particularly effective in systems wherein the random number generated at the Home System 200 is used in a manner that is insecure, such as the case when the same generated keys are used for an extended period of time.

An embodiment that protects against a rogue shell attack uses the processors and memory in the subscriber identification token to generate an electronic signature that cannot be reproduced by a mobile unit without the insertion of the subscriber identification token.

FIG. 3 illustrates an embodiment for performing local authentication of a subscriber in a wireless communication system. In this embodiment, the subscriber identification token 230 is programmed to generate an authentication response based on a key that is not passed to the mobile unit 220. Hence, if the mobile unit used by a subscriber is a rogue shell, the rogue shell cannot recreate the appropriate authentication responses.

Similar to the method described in FIG. 2, the mobile unit 220 generates a signature signal based upon an IK 310 that is received from the subscriber identification token 230 and a message that is to be sent to the VS 210. However, in one embodiment, the signature signal is not passed to the VS. The signature signal is passed to the subscriber identification token 230, and is used along with an additional key to generate a primary signature signal. The primary signature signal is sent out to the mobile unit 220, which in turn transmits the primary signature signal to the VS 210 for authentication purposes.

HS 200 generates a random number 240 and an expected response (XRES) 270 based on knowledge of the Secure Key held on the subscriber identification token 230. The random number 240 and the XRES 270 are

WO 02/096150

PCT/US02/16103

10

transmitted to the VS 210. Communication between the HS 200 and the VS 210 is facilitated in the manner described in Fig. 1. The VS 210 transmits the random number 240 to the mobile unit 220 and awaits the transmission of a confirmation message 260 from the mobile unit 220. The confirmation message 260 and the XRES 270 are compared at a compare element 280 at the VS 210. If the confirmation message 260 and the XRES 270 match, the VS 210 proceeds to provide service to the mobile unit 220.

Mobile unit 220 conveys the random number 240 to the subscriber identification token 230 that has been electronically coupled with the mobile unit 220 by the subscriber. A Secure Key 300 is stored on the subscriber identification token 230. Both the Secure Key 300 and the random number 240 are used by a key generator 250 to generate the confirmation message 260, a Cryptographic Key (CK) 290, an Integrity Key (IK) 310, and a UIM Authentication Key (UAK) 320. The CK 290 and IK 310 are conveyed to the mobile unit 220.

At the mobile unit 220, the CK 290 is used for encrypting transmission data frames (not shown in FIG. 3). The IK 310 is used to generate a signature signal 340. The signature signal 340 is the output of a signature generator 330 that uses an encryption operation or a one-way operation, such as a hashing function, upon the IK 310 and a message 350 from the mobile unit 220. The signature signal 340 is transmitted to the subscriber identification token 230. At the subscriber identification token 230, the signature signal 340 and the UAK 320 are manipulated by a signature generator 360 to generate a primary signature signal 370. The primary signature signal 370 is transmitted to the mobile unit 220 and to the VS 210, where a verification element 380 authenticates the identity of the subscriber. The verification element 380 can accomplish the verification by regenerating the signature signal 340 and the primary signature signal 370. Alternatively, the verification element 380 can receive the signature signal 340 from the mobile unit 220 and only regenerate the primary signature signal 370.

The regeneration of the signature signal 340 and the primary signature signal 370 at the VS 210 can be accomplished by a variety of techniques. In

WO 02/096150

PCT/US02/16103

11

one embodiment, the verification element 380 can receive a UAK 390 and an integrity key from the Home System 200. When the verification element 380 also receives the message 350 from the mobile unit 220, the signature signal can be generated and then be used to generate the primary signature element.

The signature generator 360 within the subscriber identification token 230 can comprise a memory and a processor, wherein the processor can be configured to manipulate inputs using a variety of techniques. These techniques can take the form of encryption techniques, hashing functions, or any nonreversible operation. As an example, one technique that can be implemented by the subscriber identification token is the Secure Hash Algorithm (SHA), promulgated in Federal Information Processing Standard (FIPS) PUB 186, "Digital Signature Standard," May 1994. Another technique that can be performed by the subscriber identification token is the Data Encryption Standard (DES), promulgated in FIPS PUB 46, January 1977. The use of the term "encryption" as used herein does not necessarily imply that operations must be reversible. The operations may be non-reversible in the embodiments described herein.

The key generator 250 can also comprise a memory and a processor. Indeed, in one embodiment, a single processor can be configured to accomplish the functions of the signature generator 360 and the key generator 250. Verification can be performed by calculating the same result from the same inputs at the verification element 380, and comparing the calculated and transmitted values.

In a more detailed description of the embodiment above, signal generator 330 can be configured to implement a technique referred to herein as HMAC-SHA-1. In the embodiment described above, it was noted that a hashing function could be used within the signal generator 330 to generate a signature signal 340. A description of hash-based MACs (HMACs) can be found in the paper, "Keying Hash Functions for Message Authentication," Bellare, et al., Advances in Cryptology - Crypto 96 Proceedings, Lecture Notes in Computer Science Vol. 1109, Springer-Verlag, 1996. An HMAC is a

WO 02/096150

PCT/US02/16103

12

MAC scheme that uses a cryptographic hash function, such as SHA-1, in a two-step process. In an HMAC-SHA-1 scheme, a random and secret key initializes the SHA-1 function, which is then used to produce a digest of the message. The key is then used to initialize SHA-1 again to produce a digest of the first digest. This second digest provides a MAC that will be appended to each message. In the embodiment described herein, the integrity key (IK) 310 that is generated by the subscriber identification token 230 can be used as the random and secret key initializing SHA-1. FIG. 4 is a flow chart illustrating the implementation of the HMAC in the mobile station, which is initialized by an integrity key from the subscriber identification token, and the implementation of the HMAC in the subscriber identification token, which is initialized by a UIM Authentication Key.

In FIG. 4, HS 200 generates a random number 240 and an expected response (XRES) 270 based on knowledge of the private information held on the subscriber identification token 230. The random number 240 and the XRES 270 are transmitted to the VS 210. Communication between the HS 200 and the VS 210 is facilitated in the manner described in Fig. 1. The VS 210 transmits the random number 240 to the mobile unit 220 and awaits the transmission of a confirmation message 260 from the mobile unit 220. The confirmation message 260 and the XRES 270 are compared at a compare element 280 at the VS 210. If the confirmation message 260 and the XRES 270 match, the VS 210 proceeds to provide service to the mobile unit 220.

Mobile unit 220 conveys the random number 240 to the subscriber identification token 230 that has been electronically coupled with the mobile unit 220 by the subscriber. A Secure Key 300 is stored on the subscriber identification token 230. Both the Secure Key 300 and the random number 240 are used by a key generator 250 to generate the confirmation message 260, a Cryptographic Key (CK) 290, an Integrity Key (IK) 310, and a UIM Authentication Key (UAK) 320. The CK 290 and IK 310 are conveyed to the mobile unit 220.

At the mobile unit 220, the CK 290 is used for encrypting transmission data frames (not shown in FIG. 4). The IK 310 is used to generate a

WO 02/096150

PCT/US02/16103

13

signature signal 340 from the signature generator 330. The signature generator 330 is configured to produce a transformation of the message 260 through the use of SHA-1. The SHA-1 hashing function is initialized by the IK 310.

5 The signature signal 340, which is the result of the SHA-1 hashing function transforming the message 260, is transmitted to the subscriber identification token 230. At the subscriber identification token 230, the signature signal 340 and the UAK 320 are manipulated by a signature generator 360 to generate a transformation of the of the signature signal 340, which is the UIM message authentication code (UMAC) 370. The signature
10 generator 360 is also configured to implement the SHA-1 hashing function. However, the function is initialized using UAK 320, rather than IK 310.

The UMAC 370 is transmitted to the mobile unit 220 and to the VS 210, where a verification element 380 authenticates the identity of the subscriber.
15 The verification element 380 can accomplish the verification by regenerating the signature signal 340 and the UMAC 370. Alternatively, the verification element 380 can receive the signature signal 340 from the mobile unit 220 and only regenerate the UMAC 370.

FIG. 5 is a flow chart illustrating a generalized description of the
20 embodiment. At step 500, a mobile unit generates a message that requires authentication. At step 501, the mobile unit receives an integrity key (IK) of length L from a subscriber identification token. At step 502, the mobile unit pads the integrity key IK to length b, wherein b is the block size of the hashing function of a signature generator within the mobile unit. In one embodiment,
25 the key can be zero-padded to length b. In another embodiment, the key can be XORed with padding constants of length b. If the IK already has length b, then this step can be omitted. At step 504, the padded IK is concatenated with the message that requires authentication. The concatenation of the padded IK and the message is then hashed at step 505 by a signature
30 generator configured to implement a hashing function such as SHA. In one embodiment, the output of the XOR operation is saved within a memory

WO 02/096150

PCT/US02/16103

14

element, and can be recalled for further use if the IK from the subscriber identification token remains the same during the communication session.

If the UIM authentication key (UAK) is to be used, then the program flow proceeds to step 510. If the UAK is not to be used, then the program
5 flow proceeds to step 520.

At step 510, the hashed message from step 505 is transmitted to the subscriber identification token. At step 511, the subscriber identification token pads the UAK to length b , unless the UAK is already of length b . The padded IK can be stored in memory for reuse when a subsequent message requires authentication during the communication session. At step 512, the padded IK
10 and the hashed message are concatenated and inputted into a signature generator. The signature generator is configured to implement a hashing function, such as SHA-1 at step 513. At step 514, the output of the signature generator is transmitted from the subscriber identification token to the mobile
15 unit.

At step 520, the same integrity key is used to rehash the already hashed message. The hashed message from step 505 is sent to a second signature generator within the mobile unit. Or alternatively, the hashed message can be re-inserted into the signature generator of step 505. If one
20 integrity key is to be used in two hashing processes, then the integrity key must be altered so that each of hashing generators is initialized with a different value. For example, for each hashing step, the integrity key can be bit-wise added to either constant value c_1 or constant value c_2 , both of length b . Using this method, only one integrity key needs to be generated by the
25 subscriber identification token.

It should be noted that the more secure embodiment is the implementation wherein the second hashing step is performed using the UAK at the subscriber identification token.

The process described in FIG. 5 can be mathematically described by
30 the equation:

$$HMAC(x) = F_{token}(UAK, F_{mobile}(IK, x)),$$

WO 02/096150

PCT/US02/16103

15

wherein $F_Y(\)$ represents a hashing function performed at a location Y, x represents the original message, UAK and IK are the keys, and a comma represents a concatenation.

5 A subscriber identification token used in a CDMA system or a GSM system, also known as an R-UIM or a USIM, respectively, can be configured to generate the primary signature signal or UMAC in the manner described above, i.e., all messages generated by the mobile unit are encrypted and authenticated. However, since the central processing unit in such tokens can
10 be limited, it may be desirable to implement an alternative embodiment, wherein a weight of importance is assigned to a message frame so that only important messages are securely encrypted and authenticated. For example, a message frame containing billing information has more need for increased security than a message frame containing a voice payload. Hence, the
15 mobile unit can assign a greater weight of importance to the billing information message frame and a lesser weight of importance to the voice message frame. When the subscriber identification token receives the signature signals generated from these weighted messages, the CPU can assess the different weights of importance attached to each signature signal and determine a
20 primary signature signal for only the heavily weighted signature signals. Alternatively, the mobile unit can be programmed to convey only the "important" signature signals to the subscriber identification token. This method of selective primary signature signal generation increases the efficiency of the subscriber identification token by lightening the processing
25 load of the subscriber identification token.

The embodiments described above prevent unauthorized use of a subscriber's account by requiring a more secure transaction between the subscriber identification token and the mobile unit. Since the mobile unit cannot generate a primary signature signal without knowledge of the secret
30 UAK, the mobile unit that is programmed to act as a rogue shell cannot misappropriate subscriber information for wrongful purposes.

WO 02/096150

PCT/US02/16103

16

The embodiments described above also maximize the processing capability of the subscriber identification token by operating on a signature signal, rather than a message. Typically, a signature signal will have a shorter bit length than a message. Hence, less time is required for the signature generator in the subscriber identification to operate on a signature signal rather than a transmission message frame. As mentioned above, the processing capability of the subscriber identification token is usually much less than the processing capability of the mobile unit. Hence the implementation of this embodiment would provide secure authentication of messages without sacrificing speed.

However, it should be noted that improvements in processor architectures occur at an almost exponential pace. Such improvements consist of faster processing times and smaller processor sizes. Hence, another embodiment for providing local authentication can be implemented wherein the primary signature signal can be generated directly from a message, rather than indirectly through a short signature signal. A mobile unit can be configured to pass a message directly to the subscriber identification token, one with the capability to generate a primary signature signal quickly, rather than passing the message to a signature generating element within the mobile unit. In another embodiment, only a limited number of messages need be passed directly to the subscriber identification token, in accordance with the degree of security needed for said messages.

It should be noted that while the various embodiments have been described in the context of a wireless communication system, the various embodiments can be further used to provide secure local authentication of any party using an unfamiliar terminal connected in a communications network.

Thus, novel and improved methods and apparatus for performing local authentication of a subscriber in a communication system have been described. Those of skill in the art would understand that the various illustrative logical blocks, modules, circuits, and algorithm steps described in connection with the embodiments disclosed herein may be implemented as

WO 02/096150

PCT/US02/16103

17

electronic hardware, software, firmware, or combinations thereof. The various illustrative components, blocks, modules, circuits, and steps have been described generally in terms of their functionality. Whether the functionality is implemented as hardware, software, or firmware depends upon the particular application and design constraints imposed on the overall system. Skilled artisans recognize the interchangeability of hardware, software, and firmware under these circumstances, and how best to implement the described functionality for each particular application.

Implementation of various illustrative logical blocks, modules, circuits, and algorithm steps described in connection with the embodiments disclosed herein may be implemented or performed with a digital signal processor (DSP), an application specific integrated circuit (ASIC), a field programmable gate array (FPGA) or other programmable logic device, discrete gate or transistor logic, discrete hardware components. A processor executing a set of firmware instructions, any conventional programmable software module and a processor, or any combination thereof can be designed to perform the functions described herein. The processor may advantageously be a microprocessor, but in the alternative, the processor may be any conventional processor, controller, microcontroller, or state machine. The software module could reside in RAM memory, flash memory, ROM memory, EPROM memory, EEPROM memory, registers, hard disk, a removable disk, a CD-ROM, or any other form of storage medium known in the art. An exemplary processor is coupled to the storage medium so as to read information from, and write information to, the storage medium. In the alternative, the storage medium may reside in an ASIC. The ASIC may reside in a telephone or other user terminal. In the alternative, the processor and the storage medium may reside in a telephone or other user terminal. The processor may be implemented as a combination of a DSP and a microprocessor, or as two microprocessors in conjunction with a DSP core, etc. Those of skill would further appreciate that the data, instructions, commands, information, signals, bits, symbols, and chips that may be referenced throughout the above description are represented by voltages, currents, electromagnetic waves,

WO 02/096150

PCT/US02/16103

18

magnetic fields or particles, optical fields or particles, or any combination thereof.

Various embodiments of the present invention have thus been shown and described. It would be apparent to one of ordinary skill in the art, however, that numerous alterations may be made to the embodiments herein disclosed without departing from the spirit or scope of the invention.

WE CLAIM:

10

WO 02/096150

PCT/US02/16103

19

CLAIMS

1. A subscriber identification module for providing local authentication of a
2 subscriber in a communication system, comprising:
3 a memory; and
4 a processor configured to implement a set of instructions stored in the
5 memory, the set of instructions for:
6 generating a plurality of keys in response to a received
7 challenge;
8 generating an initial value based upon a first key from the
9 plurality of keys;
10 concatenating the initial value with a received signal to form an
11 input value, wherein the received signal is transmitted from a
12 communications unit communicatively coupled to the subscriber
13 identification module, and the received signal is generated by the
14 communications unit using a second key from the plurality of keys, the
15 second key having been communicated from the subscriber
16 identification module to the communications unit;
17 hashing the input value to form an authentication signal; and
18 transmitting the authentication signal to the communications
19 system via the communications unit.
2. The apparatus of Claim 1, wherein hashing the input value is
2 performed in accordance with the Secure Hashing Algorithm (SHA-1).
3. The apparatus of Claim 1, wherein generating the initial value
2 comprises padding the first key.
4. The apparatus of Claim 3, wherein generating the initial value further
2 comprises adding the padded first key bit-wise to a constant value.

WO 02/096150

PCT/US02/16103

20

5. The apparatus of Claim 1, wherein the received signal is generated at
2 the communications unit by:
receiving the second key from the subscriber identification module;
4 generating a local initial value based upon the second key;
concatenating the local initial value and a message to form a local input
6 value;
hashing the local input value to form the received signal; and
8 transmitting the received signal to the subscriber identification module.
6. The apparatus of Claim 5, wherein generating the local initial value
2 comprises padding the second key.
7. The apparatus of Claim 6, wherein generating the local initial value
2 further comprises adding the padded second key bit-wise to a second
constant value.
8. A subscriber identification module, comprising:
2 a key generation element; and
a signature generator configured to receive a secret key from the key
4 generation element and information from a mobile unit, and further configured
to generate a signature that will be sent to the mobile unit, wherein the
6 signature is generated by concatenating the secret key with the information
from the mobile unit and hashing the concatenated secret key and
8 information.
9. The subscriber identification module of Claim 8, wherein the key
2 generation element comprises:
a memory; and
4 a processor configured to execute a set of instructions stored in the
memory, wherein the set of instructions performs a cryptographic
6 transformation upon an input value to produce a plurality of temporary keys.

WO 02/096150

PCT/US02/16103

21

10. The subscriber identification module of Claim 9, wherein the
2 cryptographic transformation is performed using a permanent key.
11. An apparatus for providing secure local authentication of a subscriber
2 in a communication system, comprising a subscriber identification module
configured to interact with a communications unit, wherein the subscriber
4 identification module comprises:
- a key generator for generating a plurality of keys from a received
6 value and a secret value, wherein at least one communication key from
the plurality of keys is delivered to the communications unit and at least
8 one secret key from the plurality of keys is not delivered to the
communications unit; and
- a signature generator for generating an authorization signal from
10 hashing a version of the at least one secret key together with an
authorization message, wherein the authorization message is
12 generated by the communications unit using a version of the at least
one communication key.
- 14
12. The apparatus of Claim 11, wherein the subscriber identification
2 module is configured to be inserted into the communications unit.
13. The apparatus of Claim 11, wherein the at least one communication
2 key comprises an integrity key.
14. The apparatus of Claim 11, wherein hashing is performed in
2 accordance with SHA-1.
15. A method for providing authentication of a subscriber using a
2 subscriber identification device, comprising:
- generating a plurality of keys;
- 4 transmitting at least one key from the plurality of keys to a
communications device communicatively coupled to the subscriber

WO 02/096150

PCT/US02/16103

22

- 6 identification device and holding private at least one key from the plurality of
keys;
8 generating a signature at the communications device using both the at
least one key transmitted to the communications device and a transmission
10 message, wherein generating is implemented by hashing a concatenated
value formed from the at least one key and the transmission message;
12 transmitting the signature to the subscriber identification device;
receiving the signature at the subscriber identification device;
14 generating a primary signature from the received signature, wherein
the generating is implemented by hashing a concatenated value formed from
16 the at least one private key and the signature received from the
communications device; and
18 conveying the primary signature to a communications system.
16. The method of Claim 15, wherein hashing is implemented in
2 accordance with SHA-1.
17. An apparatus for authenticating a subscriber in a wireless
2 communication system, wherein the apparatus can be communicatively
coupled to a mobile station operating within the wireless communications
4 system, comprising:
a memory; and
6 a processor configured to implement a set of instructions stored in the
memory, the set of instructions for selectively generating a primary signature
8 based upon a key that is held private from the mobile station and a secondary
signature that is received from the mobile station.

WO 02/096150

PCT/US02/16103

1/5

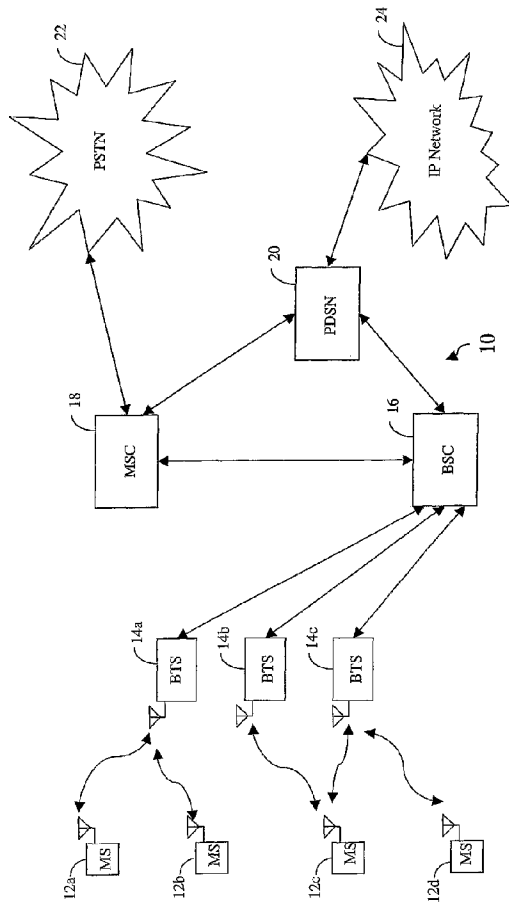


FIG. 1

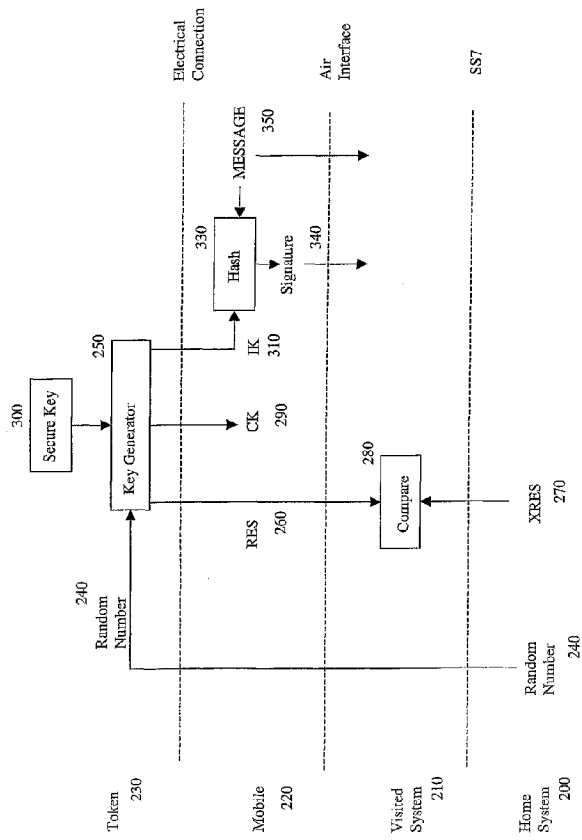


FIG. 2

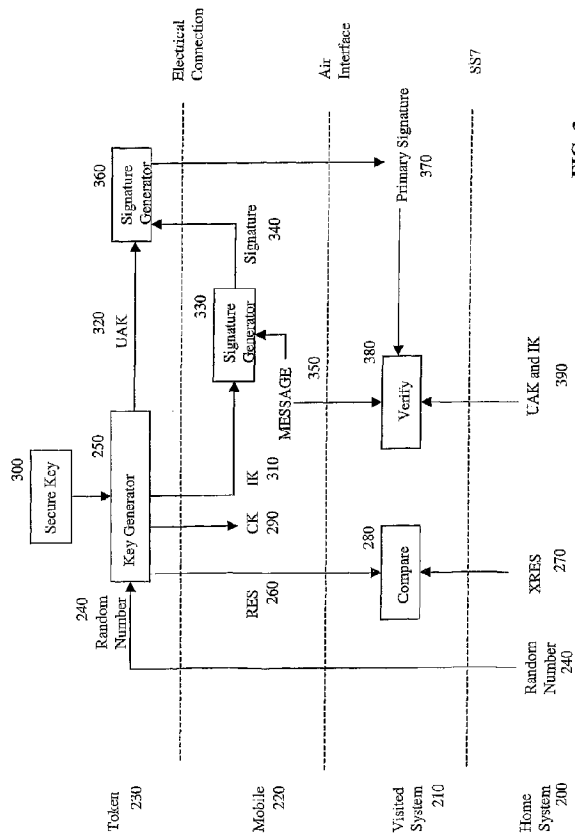


FIG. 3

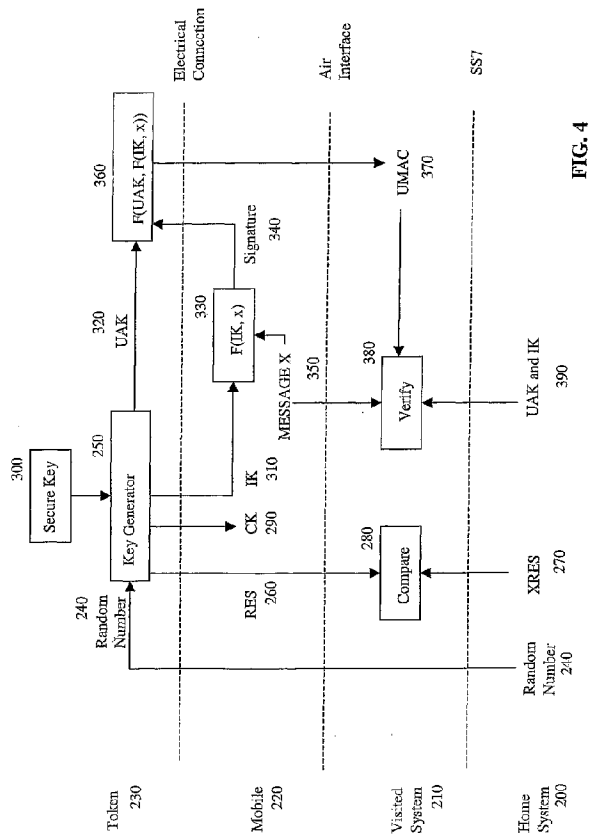


FIG. 4

WO 02/096150

PCT/US02/16103

5/5

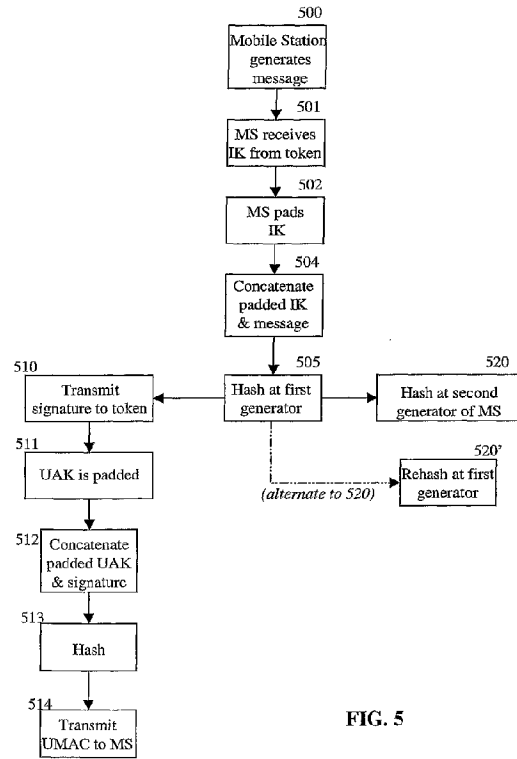


FIG. 5

INTERNATIONAL SEARCH REPORT

International Application No.

PCT/US 02/6103

A. CLASSIFICATION OF SUBJECT MATTER

IPC 7 H04Q7/38

H04L9/32

H04L29/06

H04Q7/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 H04Q H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the International search (name of data base and, where practical, search terms used)

EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category * Citation of document, with indication, where appropriate, of the relevant passages

Relevant to claim No.

X

"Rouges MS_Shell Treat Analysis"
3GPP TSG SA W63 SECURITY, 'Online!
28 - 30 November 2000, pages 1-17,
XP002210348
Sophia Antipolis, France
Retrieved from the Internet:
<URL:http://www.3gpp.org/ftp/tsg_sa/W63_Se
curity/2000_meetings/TS653_16_Sophia_Antip
olis/Docs/PDF/S3-000711.pdf>
retrieved on 2002-08-20

8-10

A

paragraph '02.2!
paragraph '2.4.4!
paragraph '05.2!

1-7,
11-17

-/-

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Species categorization of cited documents:

A document falling in the general class of the A which is of
considerable to be of particular relevance

E earlier document but published on or after the international
filing date

T document which may throw doubts on priority claim(s) or
which is cited to establish the publication date of another
claim or other special reason (as specified)

C document relating to an oral disclosure, use, exhibition or
other means

P document published prior to the international filing date but
later than the priority date claimed

I is a document published after the international filing date
on priority date and not in conflict with the applicable law
designed to understand the prior art or theory underlying the
invention

X document of particular relevance; the claimed invention
cannot be considered novel or cannot be considered to
involve an inventive step when the document is taken into
account

Y document of particular relevance; the claimed invention
cannot be considered to involve an inventive step when the
document is considered with one or more other such docu-
ments, such combination being obvious to a person skilled
in the art

S document number of the same patent family

Date of the actual completion of the international search

Date of mailing of the international search report

23 August 2002

05/09/2002

Name and mailing address of the ISA

Authorized officer

European Patent Office, P.O. Box 6818 Paterlaan 2
NL-2200 HV Haarlem
Tel: (+31-70) 345-2000, Tx 31 651 opt 4
Fax: (+31-70) 340-2016

Figiel, B

Form BGT (SA/219 (Security) (Rev. 1)) (July 1992)

INTERNATIONAL SEARCH REPORT		In Application No PCT/US 02/16103
C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT		
Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	ALBERT LEVI, M. UFUK CAGLAYAN: "A Multiple Signature Based Certificate Verification Scheme" BOGAZICI UNIVERSITY, 'Online! XP002210349 Istanbul Retrieved from the Internet: <URL:http://citeseer.nj.nec.com/cache/papers/cs/2506/http:zSzzSzmercan.cmpe.boun.edu.tr/zSzllevizSzbas98.pdf/a-multiple-signature-based.pdf> 'retrieved on 2002-08-20! abstract paragraph '0001! -----	1
A	"Incorporating UIM into 3G and IMT-2000 Systems" TIA/EIA/IS-808, 'Online! - November 2000 (2000-11) XP002210350 Retrieved from the Internet: <URL:http://www.tiaonline.org/standards/sfg/imt2k/cdma2000/TIA-EIA-IS-808.pdf> 'retrieved on 2002-08-20! page 7 -page 25 -----	1-7
A	MEHROTRA A ET AL: "MOBILITY AND SECURITY MANAGEMENT IN THE GSM SYSTEM AND SOME PROPOSED FUTURE IMPROVEMENTS" PROCEEDINGS OF THE IEEE, IEEE. NEW YORK, US, vol. 86, no. 7, July 1998 (1998-07), pages 1480-1497, XP000854168 ISSN: 0018-9219 the whole document -----	1-7
E	WO 02 054663 A (QUALCOMM INC) 11 July 2002 (2002-07-11) page 12, line 7-13; figure 3 -----	8-14,17

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No.
PCT/US 02/16103

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 02054663	A	US 2002081931 A1	11-07-2002
		WO 02054663 A2	11-07-2002
		US 2002081933 A1	11-07-2002

フロントページの続き

(81)指定国 AP(GH,GM,KE,LS,MW,MZ,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,MD,RU,TJ,TM),EP(AT, BE,CH,CY,DE,DK,ES,FI,FR,GB,GR,IE,IT,LU,MC,NL,PT,SE,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,ML,MR,NE,SN, TD,TG),AE,AG,AL,AM,AT,AU,AZ,BA,BB,BG,BR,BY,BZ,CA,CH,CN,CO,CR,CU,CZ,DE,DK,DM,DZ,EC,EE,ES,FI,GB,GD,GE, GH,GM,HR,HU,ID,IL,IN,IS,JP,KE,KG,KP,KR,KZ,LC,LK,LR,LS,LT,LU,LV,MA,MD,MG,MK,MN,MW,MX,MZ,NO,NZ,OM,PH,P L,PT,RO,RU,SD,SE,SG,SI,SK,SL,TJ,TM,TN,TR,TT,TZ,UA,UG,UZ,VN,YU,ZA,ZM,ZW

(74)代理人 100084618

弁理士 村松 貞男

(74)代理人 100092196

弁理士 橋本 良郎

(72)発明者 クイック、ロイ・エフ・ジュニア

アメリカ合衆国、カリフォルニア州 92107、サン・ディエゴ、バルセロナ・ドライブ 1150

(72)発明者 ローズ、グレゴリー・ジー

オーストラリア国、ニュー・サウス・ウェールズ州 2137、モルトレイク、キングストン・アベニュー 6

Fターム(参考) 5J104 AA07 KA01 KA03 KA04 NA02 NA05 NA12 NA38 PA01

5K051 CC07 HH01 HH17

5K067 AA30 BB04 BB21 DD51 EE02 EE10 HH36